Internal Audit progress report – December 2016

The purpose of this report is to advise the Audit Committee of our progress in planning and delivering the 2016-17 Internal Audit Plan.

Progress to date

Since the Audit Committee last met, we have completed the Fines Recovery review. The reviews of Cryptographic Controls and phase one of the IT Asset Management, the reports are being finalised with management.

Reviews planned

Planning for the Investigations, Data Protection law reform project and Stakeholder reviews has started.

The Investigations review will be carried out in December with the IT Asset Management (phase 2) and Data Protection law reform projects being undertaken in January. The Stakeholder review will be carried out in February 2017, with timing to be agreed with management. The annual follow-up review is planned for February / March 2017.

Status and progress of reviews

Completed reviews

Recovery of Monetary Penalties

During 2015-16, the ICO issued a total of 22 final notices, with a total value of £2.5 million. However, by the end of quarter 2 2016-17, 16 final notices with a total value just over £2 million have been levied. In addition, the majority of penalties were levied against public bodies and therefore payment was not considered to be a risk. A greater number of penalties are being issued against commercial organisations, some of whom are run by unscrupulous individuals who fail to pay the penalties levied and need to be more proactively managed.

We found that although responsibility for recovery of penalties has moved to Enforcement, the process was working well. We identified two opportunities to improve the process further; firstly, to document the process and identify roles and responsibilities and secondly there was a lack of reporting of the status and progress of penalty recovery. Reporting will become a key monitoring control as the number of penalties is likely to increase, ICO management need to be made aware of the current status and progress of recoveries to ensure the focus is on the appropriate areas.

Finalising reports

The reports for the following reviews are being agreed and finalised with management:

Cryptographic controls

The review was to confirm that the activities carried out by the ICO over devices that are designated Accountable Security (ACCSEC) devices would meet the requirements from CESG. We were able to confirm that the design over the new process provides governance that ensures management and the senior management team are informed of progress of the audit and compliance activities over ACCSEC devices. The review identified opportunities to improve the design of the processes but no fundamental changes were required.

Going forward (beyond 2017), there is the possibility that the formal CESG process will not be required. However, it is managements intention to retain the process over the annual auditing and reporting of ACCSEC devices in order to ensure appropriate governance is in place.

IT Asset Management – Phase One

As a result of changes to the process over the governance over ACCSEC devices (see Cryptographic controls update), the ICO has taken the opportunity to review the process in place over IT assets and how they are managed. The review of IT Asset Management has been split into two phases; the first phase is to review the design of the amended processes in place over IT assets and the second is to establish how those controls are operating.

The conclusion of the first phase is to that the processes have been designed appropriately and should ensure that IT assets are identified, periodically checked and records updated. The recommendations should further improve the processes being brought in.

People Strategy

The ICO is facing a significant change in the services that the organisation is expected to deliver. The impact of implementing Data Protection law reform in 2018 will require the ICO to deal with the potential of the corporate and private sector reporting more data breaches. The ICO will need to be able to deal with the expected increase in investigations as well as preparing for legislation that brings the UK in line with the General Data Protection Regulation from the EU.

The ICO has established a People Strategy and a Recruitment Strategy in preparation of the changes in the future. The People Strategy sets out six goals that will make the ICO a 'Great place to work and develop'. However, we found that there was a lack of sufficient detailed planning to establish whether the ICO has sufficient time to recruit, train make changes to the organisation to be ready for the changes to Data Protection law. Whilst there has been uncertainty created by the vote by the UK to leave the EU, and lack of clarity by the UK government on the budget impact on the ICO, more detailed planning over limited scenarios would allow the ICO to assess the risks the organisation may face to meet its new obligations.

Reviews in progress

Investigations

Initial planning meeting has been held and a draft audit planning brief is with management for review. The fieldwork will be completed in December with a report expected to be issued in January.

Data Protection law reform

Discussion on the review scope and timing has been held with management. The review will focus on the project governance to deliver the necessary outcomes to support the transition to new legislation and the changes to the ICO required to meet its obligations for new Data Protection legislation. The review timing has yet to be agreed with management. The audit planning brief will be drafted in December with a view to agreeing the audit brief before the Christmas holiday break.

Follow up review

The annual follow-up review of management actions that have been actioned during 2016-17 period, will be carried out in February / March 2017. The report is expected to be issued in mid-March.

Stakeholders

Initial planning meetings have been scheduled in December to agree the scope and timing of the review into Stakeholder management and engagement. The review will be carried out in during early February subject to agreement with management. The intention is to have the report ready for the March 2017 Audit Committee.

Overall summary of plan progress

Review	Scope	Timing	Days	Progress
Fines recovery	Review the process in place to recover fines issued to organisations that remain unpaid. The review will are cover how unpaid fines are identified, performance measures of fine payment are reported and the success of follow up activities to recover fines to ensure this process is efficient and effective.	Q2	6	Completed
Cryptographic Controls	CESG have defined a process to manage cryptographic controls to ensure encrypted data remains available if encryption keys become unavailable (through loss or corruption). The ICO are required to comply and demonstrate compliance by self-assessment. The audit will provide assurance over the compliance process to ensure that the self-assessment is robust and appropriate supervision is in place.	Q2	4*	Reporting
GDPR project "Data Protection law reform project"	Provide assurance over the project to manage the impact of GDPR on the ICO, including governance over the change programme and interactions with other parts of the ICO. The review will include how the ICO have resourced the project and the activity to backfill project members' roles and the recruitment for the new activities as ICO takes responsibility for GDPR.	Q3	8	Planning
IT Asset Management	Management are establishing policy and procedure to manage IT assets. The review will be delivered in two phases: 1. Review the policy and procedures to ensure the design of controls are likely to manage IT assets to ensure records are complete, accurate and will be kept up to date. 2. Once the procedures have been deployed, a second review will evaluate the controls in place and operating as expected.	Q2	11*	Phase 1 – reporting Phase 2 - planning
Investigations	The review will cover how the ICO manages investigations through communication with stakeholders, the use of frameworks, gathering intelligence and finally reporting on investigations. Where possible, we will benchmark against other regulators management of investigations.	Q3	9	Planning – fieldwork in December
People Strategy	People are a key part of the ICO and the management have established that the organisation needs to ensure it has "the right people, in the right place at the right time". The review will consider how staff performance is managed across the organisation and that managers are properly prepared to implement performance management to ensure consistency. The review will also consider the progress of recommendations made from the staff performance review in 2015-16.	Q3	8	Reporting
Stakeholder engagement	ICO is tasked with communicating key messages on data protection (and in the future data privacy) and access to information. A review will establish how those communications are prepared and published including thought leadership. The focus will be on how strategic activity is determined, agreed and approved, including consideration of the impact of GDPR on these activities. The review will also determine how the target audience is selected and the medium to use. How the ICO measures the success of such communication will also be assessed.	Q4	11.5	Planning – scheduled for February
Follow Up	Review of the arrangements to capture and implement audit recommendations in a timely manner.	Q4	3.5	Planning – scheduled for January

* Additional review / budget agreed with management

www.grant-thornton.co.uk